Omgevingsdienst Zuid-Holland Zuid

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 170

9 juli

2015

Officiële uitgave van gemeenschappelijke regeling
Omgevingsdienst Zuid-Holland Zuid.

Regeling gebruik ICT middelen en informatie van de werkgever Drechtsteden/Zuid-Holland Zuid

Het dagelijks bestuur van de gemeenschappelijke regeling Omgevingsdienst Zuid-Holland Zuid,

Gelet op:
- Artikel 160 Gemeentewet;
- De nota Integriteitsbeleid en de Gedragscode Drechtsteden/Zuid-Holland Zuid oktober 2014;
- Artikel 8 lid 4 van “Regeling Netwerk Georganiseerd Overleg Drechtsteden” en
- Artikel 4 lid 2 van “Overeenkomst tot vaststelling van een uniforme rechtspositieregeling voor de gemeenschappelijke regeling Drechtsteden, mede ten behoeve van de gemeenten Alblasserdam, Dordrecht, Hendrik Ido Ambacht, Papendrecht, Sliedrecht, Zwijndrecht en de gemeenschappelijke regelingen, Dienst Gezondheid en Jeugd Zuid-Holland Zuid en Omgevingsdienst Zuid-Holland Zuid.

Gezien de instemming van de medezeggenschap d.t.v. het Netwerk van Ondernemingsraden Drechtsteden d.d 26 mei 2015.

Besluit:

Vast te stellen de hierna volgende

Regeling gebruik ICT middelen en informatie van de werkgever Drechtsteden / Zuid-Holland Zuid

Hoofdstuk I WERKINGSSFEER EN BEGRIPPENKADER

Artikel 1

Deze regeling is voor alle medewerkers van toepassing op het gebruik van ICT-middelen en informatie van de werkgever, ongeacht de plaats waar dit plaatsvindt en ongeacht het eigendom van de middelen waarmee de informatie wordt benaderd. Tevens is deze regeling van toepassing op de wijze waarop controle op dit gebruik plaatsvindt.

Artikel 2

In deze regeling wordt verstaan onder:

Werkgever:

a. Voor de medewerkers van de gemeenten Alblasserdam, Dordrecht, Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht en Zwijndrecht: het college van burgemeester en wethouders van de desbetreffende gemeente;
b. Voor het griffiepersoneel werkzaam bij één van de bovengenoemde gemeenten: de gemeenteraad;
c. Voor de medewerkers van de Gemeenschappelijke regeling Drechtsteden, de gemeenschappelijke regeling Dienst Gezondheid & Jeugd Zuid-Holland Zuid en de Gemeenschappelijke regeling Omgevingsdienst Zuid-Holland Zuid: het dagelijks bestuur van de desbetreffende gemeenschappelijke regeling.

Medewerker: degene die bij een van de werkgevers in het netwerk [voetnoot: met het netwerk worden de organisaties bedoeld: de gemeenten Alblasserdam, Dordrecht, Hendrik Ido Ambacht, Papendrecht, Sliedrecht en Zwijndrecht en de gemeenschappelijke regelingen Drechtsteden, Dienst Gezondheid & Jeugd Zuid-Holland Zuid en de Omgevingsdienst Zuid-Holland Zuid] onder welke titel en hoedanigheid ook, werkzaam is (geweest) of werkzaamheden (heeft) verricht.

Werkplek: iedere plaats die in verband met het verrichten van arbeid wordt gebruikt.

Persoonsgegeven: een gegeven dat herleidbaar is tot een geïdentificeerde of identificeerbaar natuurlijk persoon.

ICT middelen: alle huidige en toekomstige elektronische informatie- en communicatie faciliteiten en ICT-apparatuur (zoals Smartphones, Tablets, Laptops, USB geheugensticks) door of namens de werkgever aan medewerkers beschikbaar gesteld, alsmede de privé ICT-middelen indien en voor zover zij gebruikt worden op de werkplek en/of voor de uitvoering van de door of namens de werkgever opgedragen taken.

Informatie van de werkgever: alle bestanden en informatie door of namens de werkgever aan medewerkers beschikbaar zijn gesteld, hieronder begrepen informatie van de werkgevers in het netwerk;

Systeemnetwerk van de werkgever: Gemeenschappelijke Regionale Infrastructuur Drechtsteden (GRID);

Verkeersgegevens: tijdstippen, adressen, datahoeveelheid en duur van het gebruik van de ICT middelen;

Zakelijk gebruik: gebruik van de ICT middelen alsmede de faciliteiten en digitale bestanden van de werkgever ten behoeve van de functie-uitoefening door de medewerker, ongeacht de herkomst van het ICT middel.

Hoofdstuk II GEBRUIK VAN DE ICT MIDDELEN EN DE INFORMATIE VAN DE WERKGEVER

Artikel 3

1. De medewerker ontvangt een strikt persoonlijke inlogcode voor de GRID infrastructuur. Het is niet toegestaan deze inlogcode af te geven aan derden (collega's, leidinggevende of anderen) of deze met collega's te delen. Dit vanuit zowel de richtlijnen voor informatiebeveiliging als de geldende licentievoorwaarden van de achterliggende leveranciers.

2. Medewerkers gebruiken de ICT-middelen primair en hoofdzakelijk voor het uitvoeren van de aan hen opgedragen taken, in overeenstemming met wet- en regelgeving en het doel waarvoor de middelen en informatie zijn verstrekt.

3. Het is de medewerker toegestaan gebruik te maken van privé ICT middelen voor de uitvoering van de opgedragen taken. Wanneer de medewerker gebruik maakt van informatie van de werkgever dient hij zich te houden aan de bepalingen van deze regeling.

4. Incidenteel privégebruik van de ICT middelen tijdens het werk is toegestaan, mits dit niet storend is voor de dagelijkse eigen werkzaamheden en/of die van andere medewerkers.

5. Incidenteel gebruik van de door de werkgever verstrekte middelen (zoals mobiele telefoon) voor privé doeleinden is toegestaan mits binnen redelijke grenzen.

6. Medewerker dient bij het gebruik van de ICT-middelen en de informatie van de werkgever de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de werkgever te waarborgen.

7. De medewerker verschaft zich uitsluitend toegang tot die gegevens waartoe hij geautoriseerd is.

8. De informatie van de werkgever mag slechts verstrekt worden aan daartoe geautoriseerde anderen.

9. Privégebruik van de informatie en gegevens van de werkgever is niet toegestaan.

10. Het is de medewerker niet toegestaan de ICT middelen, door de werkgever ter beschikking gesteld te gebruiken:

a. voor het bezoeken van sites of voor berichtenverkeer met een pornografische, racistische, discriminerende, intimiderende, beledigende of aanstootgevende inhoud of gerelateerd aan ongewenst gedrag of sites voor berichtenverkeer die (kunnen) aanzetten tot haat en/of geweld;
b. om de werkgever en/of zijn medewerkers in diskrediet te brengen of anderszins te beschadigen;
c. om met behulp van e-mail faciliteiten kettingbrieven te versturen:
d. om met behulp van e-mail faciliteiten berichten aan alle of vrijwel alle medewerkers van de werkgever tegelijkertijd te versturen, tenzij hiervoor door de werkgever steeds afzonderlijk toestemming voor is verleend;
e. voor commerciële doeleinden, met uitzondering van de daarvoor speciaal door de werkgever ingerichte intranetsite (vraag en aanbod);
f. om zich ongeoorloofd toegang tot niet-openbare bronnen te verschaffen;
g. om voor privédoeleinden (illegale) software, films of muziek te downloaden; betaaldiensten af te nemen, online te gokken of te gamen.
h. om deel te nemen aan internet-, sms- of belspelletjes.

11. Het is de medewerker niet toegestaan met behulp van de ICT-middelen grote hoeveelheden software en bestanden te verzenden of op te vragen via het systeemnetwerk van de werkgever, waarvan de medewerker redelijkerwijs moet aannemen dat deze bestanden te omvangrijk zijn.

12. Het verbod op ongewenst gebruik zoals bedoeld in lid 10 en 11 in de (fysieke) kantooromgeving geldt ook als dat via de privé ICT middelen plaatsvindt.

13. Niet toegestane e-mail en internetgebruik wordt zo veel mogelijk door de afdeling ICT softwarematig onmogelijk gemaakt

14. Medewerker dient schade aan, verlies of diefstal van de ICT-middelen of de informatie van de werkgever onverwijld bij de leidinggevende en de afdeling ICT te melden. Bij verlies of diefstal dient de medewerker bovendien aangifte te doen bij het bevoegd gezag.

15. De werkgever is gerechtigd specifieke instellingen op bepaalde door de werkgever verstrekte ICT middelen (bijvoorbeeld smartphones en tablets) af te dwingen en/of het gebruik van bepaalde toepassingen (apps) te blokkeren.

16. Voor het werken op afstand en het gebruik van privémiddelen geldt dat:

a. illegale software mag niet worden gebruikt voor de uitvoering van het werk.
b. er bestaat geen plicht de eigen computer te beveiligen, maar de informatie van de werkgever daarop wel.
c. Voor het werken met bepaalde toepassingen en/of gegevens (zoals het raadplegen van het BPS) is het gebruik van werken op afstand niet toegestaan.

HOOFDSTUK III TOEGANG TOT EN BEVEILIGING VAN DE INFORMATIE VAN DE WERKGEVER

Artikel 4

1. Medewerker dient de gestelde beveiligingseisen ten aanzien van de ICT middelen en de informatie van de werkgever in acht te nemen. Dit geldt zowel voor de door de werkgever ter beschikking gestelde ICT middelen als voor de informatie van de werkgever op de privé ICT middelen waarmee wordt gewerkt.

2. De medewerker is verplicht deel te nemen aan de training(en)/instructie workshops die door de werkgever worden aangeboden in het kader van de informatiebeveiliging.

3. De medewerker neemt passende technische en organisatorische maatregelen om de Informatie van de werkgever te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:

a. de beveiligingsclassificatie van de informatie;
b. de door de werkgever gestelde beveiligingsvoorschriften (o.a. informatiebeveiligingsbeleid);
c. aan de werkplek verbonden risico's;
d. het risico door het benaderen van gemeentelijke informatie met andere dan door de werkgever verstrekte of goedgekeurde ICT-apparatuur.

4. Ten behoeve van het gebruik van de ICT middelen ontvangt de medewerker van de werkgever een of meerdere persoonlijke toegangscode(s) met wachtwoord(en). De medewerker is zelf verantwoordelijk voor de vertrouwelijkheid van deze code(s) en wachtwoord(en).

5. In geval van dienstbelang en/of bij langdurige afwezigheid van de medewerker heeft de werkgever de mogelijkheid zich de toegang te verschaffen, via de afdeling ICT van het SCD, tot de digitale bestanden van de desbetreffende medewerker.

6. Het verzoek tot inzage in digitale bestanden zoals bedoeld in het voorgaande lid wordt schriftelijk gedaan en met redenen omkleed door de direct leidinggevende met toestemming van de naast hogere leidinggevende. Voordat het verzoek wordt gedaan wordt er bij het hoofd P&O van het SCD advies ingewonnen Het verzoek wordt bij het hoofd van de afdeling ICT ingediend.

7. De medewerker kan niet de toegang tot zijn e-mailaccount geweigerd worden, tenzij gegronde redenen aanwezig zijn.

8. Bij beëindiging van het dienstverband en/of inhuur worden alle ICT middelen van de werkgever geretourneerd door de medewerker zelf of zijn/haar leidinggevende. Autorisaties worden in opdracht van de leidinggevende geblokkeerd. Tevens zorgt de leidinggevende ervoor dat de bestanden (waar onder ook email) van de vertrekkende medewerker aan een door die leidinggevende nader aan te wijzen medewerker worden overgedragen.

9. Zonder uitdrukkelijke toestemming van de leidinggevende respectievelijk opdrachtgever is het vertrekkende medewerkers en andere voormalige gebruikers niet toegestaan om kopieën van bestanden en mailboxen te maken voor gebruik na het einde van het dienstverband..

10. De toegang tot het netwerk wordt vanaf datum uitdienst geblokkeerd. De persoonlijke toegangscode(s) met wachtwoord(en) en de digitale bestanden worden uiterlijk 6 maanden na de datum waarop het dienstverband is beëindigd, verwijderd. Dit tenzij er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik. In dat geval worden de gegevens bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een betrokkene noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen jegens de ex medewerker worden de gegevens alsnog verwijderd.

Hoofdstuk IV CONTROLE

Artikel 5 Controle algemeen

1. Controle door of in opdracht van de werkgever op het gebruik van de ICT-middelen en de informatie van de werkgever vindt slechts plaats in het kader van de onder lid 3 genoemde doeleinden. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle.

2. Controle vindt als regel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen.

3. De controle door de werkgever op het gebruik van de ICT-middelen en de informatie van de werkgever vindt plaats met als doel:

a. het verkrijgen van inzicht in de aard en mate van het gebruik van de ICT-middelen en de informatie van de werkgever;
b. het voorkomen van onrechtmatig gebruik dan wel misbruik van de ICT-middelen en informatie van de werkgever;
c. het beveiligen van het systeem, het netwerk, de informatie van de werkgever;
d. tegengaan van seksuele intimidatie, pesten en discriminatie en andere vormen van ongewenst gedrag;
e. het beschermen van de integriteit en goede naam van de werkgever;
f. het beheer van de ICT-middelen en toegang tot de informatie van de werkgever;
g. kosten- en capaciteit beheersing van het gebruik van ICT-middelen.

Artikel 6 Gerichte controle

1. Indien een medewerker wordt verdacht van het overtreden van deze regeling, kan gedurende een vastgestelde periode gerichte controle plaatsvinden.

2. Deze gerichte controle wordt slechts uitgevoerd nadat de medewerker is ingelicht dat signalen hierover zijn ontvangen en om zijn reactie is gevraagd. Werkgever kan deze inlichtingenplicht buiten beschouwing laten voor zover dit noodzakelijk is voor de in artikel 432 van de Wet bescherming persoonsgegevens genoemde belangen. In dit geval worden betrokkenen altijd wel zo spoedig mogelijk geïnformeerd over de gerichte controle.

3. Controle beperkt zich in principe tot verkeersgegevens van het gebruik van de ICT-middelen en de informatie van de werkgever. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats. Privé-bestanden worden hierbij zoveel mogelijk ontzien.

4. Het verzoek tot controle wordt schriftelijk gedaan en met redenen omkleed door de direct leidinggevende met toestemming van de naast hogere leidinggevende. Voordat het verzoek wordt gedaan wordt er bij het hoofd P&O van het SCD advies ingewonnen. Het verzoek wordt bij het hoofd van de afdeling ICT ingediend.

5. Medewerkers ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.

6. E-mailberichten van leden van de ondernemingsraad en vertrouwenspersonen mogen door, dan wel namens de werkgever niet inhoudelijk worden gecontroleerd. Dit geldt eveneens voor andere medewerkers die op grond van hun functie en/of bijzondere taak zich op vertrouwelijkheid kunnen beroepen. Dit geldt niet voor de controle als genoemd in art 5 lid 1.

7. De functionarissen belast met het beheer van de bestanden en de controle zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Hoofdstuk V SANCTIES

Artikel 7

1. Het overtreden van deze regeling kan voor de door de werkgever aangestelde medewerker de in hoofdstuk 16 van de CAR/UWO bedoelde rechtspositionele consequenties hebben.

2. Het overtreden van deze regeling kan voor de door de werkgever niet-aangestelde medewerker resulteren in:
a. het door de werkgever treffen van maatregelen ten behoeve van het op de medewerker verhalen van schade die door de gepleegde overtreding door de werkgever is geleden
b. het (op staande voet) beëindigen van de verhouding op basis waarvan de medewerker werkzaamheden voor de werkgever verricht.
c. een combinatie van de onder a en b genoemde maatregelen.

Hoofdstuk VI SLOTBEPALINGEN

Artikel 8

1. Wanneer er zich in het kader van deze regeling situaties voordoen waarin niet voorzien wordt, wordt conform de geldende wet- en regelgeving en in overleg met de Ondernemingsraad gehandeld.

2. De werkgever is gerechtigd om na het in werking treden van deze regeling nadere vormen van niet toegestaan gebruik van de ICT middelen af te kondigen.

Artikel 9

1. Deze regeling treedt in werking na bekendmaking en werkt terug tot en met 1 mei 2015.
2. Deze regeling wordt aangehaald als: Regeling gebruik ICT middelen en informatie van de werkgever Drechtsteden Zuid-Holland Zuid 2015.

Aldus vastgesteld door het dagelijks bestuur van de Omgevingsdienst Zuid-Holland Zuid op 25 juni 2015.

Secretaris,
Mr. R. Visser

Voorzitter,
Mr. R.A. Janssen